Claims

1. A method for migrating from a source user authenticator having a source datastore, containing encrypted password data and other unencrypted data wherein the data represents data for multiple users each having an identification and an associated password, to a target user authenticator having a target datastore comprising:

Read selected unencrypted data from source datastore;

Convert unencrypted data to be compatible with target datastore;

Populate target datastore with the converted data;

Receive an identification from a user seeking access to information protected by the target user authenticator;

Locate the corresponding identification in the target datastore and determine whether the target datastore includes a password associated with the identification;

Receive a password from the user associated with the received identification;

If the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator;

Monitor the source user authenticator for an approval response;

On receipt of an approval response from the source user authenticator populate the target datastore with the received password associating the received password with the corresponding identification;

Authenticate the identification and password using the target user authenticator.

2. The method of claim 1 further comprising the action of:

If, after determining whether the target datastore includes a password associated with the identification, the target datastore does include a password associated with the identification, then authenticate the identification and password using the target user authenticator.

3. The method of claim 1, wherein the actions of receiving a password from a user further comprises:

Receiving a password in a single submission from the user in conjunction with receiving the identification from the user.

4. The method of claim 1, wherein the action of receiving a password from a user further comprises:

Receiving a password in a submission from the user after the initial submission of the identification from the user.

5. The method of claim 1, wherein the action of receiving a password from a user further comprises:

Prompting for and receiving a password from the user after the initial submission of the identification from the user.

6. The method of claim 1, wherein the action of receiving a password from a user further comprises:

Prompting for and receiving the identification and a password from the user after the initial submission of the identification from the user.

7. The method of claim 6, wherein the action of prompting for and receiving the identification and a password from the user after the initial submission of the identification from the user occurs after determining that the target datastore does not include a password associated with the identification; and,

wherein the action further comprises using the source user authenticator to prompt for and receive the identification and a password from the user after the initial submission of the identification from the user.

8. The method of claim 7, wherein while the source user authenticator is receiving the submitted password from the user, capturing the password provided by the user in response to the source authenticator prompting and using the captured password as the received password.

9. The method of claim 7, wherein after receipt of an approval response from the source user authenticator, capturing the password provided by the user in response to the source authenticator prompting and using the captured password as the received password.

10. The method of claim 1, wherein the target datastore is an LDAP compliant directory service.

11. The method of claim 1, wherein the target datastore is a relational database.

12. The method of claim 10, wherein the source datastore is a relational database.

13. The method of claim 11, wherein the source datastore is a relational database.

14. The method of claim 1, wherein the user is a person.

15. The method of claim 1, wherein the user is a software object.

16. A method for populating password data to a target datastore of a target user authenticator after migration from a source user authenticator having a source datastore, while also responding to user requests for information comprising:

intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator;

prompting the user for an identification;

receiving the identification from the user.

locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification;

if the target datastore does not include a password associated with the identification, then:

allowing the original intercepted request to go through to the source user authenticator;

using the source user authenticator to prompt for and receive the identification and a password from the user;

capturing the password provided by the user in response to the source authenticator prompting and using the captured password as the received password

monitoring the source user authenticator for an approval response;

on receipt of an approval response from the source user authenticator populate the target datastore with the received password associating the received password with the corresponding identification;

authenticate the identification and password using the target user using the target user authenticator.

17. The method of claim 16, wherein after populating the target datastore, further comprising prompting for and receiving from the user the password associated with the identification.

18. The method of claim 17, wherein the action of prompting for and receiving from the user the password associated with the identification comprises prompting for and receiving from the user the identification and the password associated with the identification.

19. A method for checking for populated password data to a target datastore of a target user authenticator after migration from a source user authenticator having a source datastore, while also responding to user requests for information comprising:

intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator;

prompting the user for an identification;

receiving the identification from the user.

locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification;

if the target datastore does include a password associated with the identification, then:

authenticating the identification and password using the target user using the target user authenticator.

20. The method of claim 19, wherein after determining that target datastore does include a password associated with the identification further comprising prompting for and receiving from the user the password associated with the identification.

21. The method of claim 20, wherein the action of prompting for and receiving from the user the password associated with the identification comprises prompting for and receiving from the user the identification and the password associated with the identification.

22. A method for populating password data to a target datastore of a target user authenticator after migration from a source user authenticator having a source datastore, while also responding to user requests for information comprising:

intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator;

prompting the user for an identification;

receiving the identification from the user.

locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification;

if the target datastore does not include a password associated with the identification, then:

allowing the original intercepted request to go through to the source user authenticator;

using the source user authenticator to prompt for and receive the identification and a password from the user;

monitoring the source user authenticator for an approval response;

on receipt of an approval response from the source user authenticator capturing the password provided by the user in response to the source authenticator prompting and using the captured password as the received password

populate the target datastore with the received password associating the received password with the corresponding identification;

authenticate the identification and password using the target user using the target user authenticator.

23. The method of claim 22, wherein after populating the target datastore, further comprising prompting for and receiving from the user the password associated with the identification.

24. The method of claim 23, wherein the action of prompting for and receiving from the user the password associated with the identification comprises prompting for and receiving from the user the identification and the password associated with the identification.